대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2003년 제 0076554 호
Application Number 10-2003-0076554

출 원 년 월 일 : 2003년 10월 31일
Date of Application OCT 31, 2003

출 원 인 : 삼성전자주식회사 외 5명
Applicant(s) SAMSUNG ELECTRONICS CO., LTD., et al.

2004 년 11 월 15 일

특 허 청
COMMISSIONER

【서지사항】

서류명】	특허출원서
접리구분】	특허
수신처】	특허청장
출원일자】	2003.10.31
발명의 명칭】	IEEE 802.16 프라이버시 계층에서 SS 인증을 위한 EAP 프레임워크 수용 방법
발명의 영문명칭】	Acceptance method of EAP framework for SS authorization in IEEE 802.16 privacy layer
출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
대리인】	
【명칭】	유미특허법인
【대리인코드】	9-2001-100003-6
【지정된변리사】	이원일
【포괄위임등록번호】	2001-038431-4
발명자】	
【성명의 국문표기】	박애순
【성명의 영문표기】	PARK,AE SOON
【주민등록번호】	640920-2401130
【우편번호】	305-755
【주소】	대전광역시 유성구 어은동 한빛아파트 138동 301호
【국적】	KR
발명자】	
【성명의 국문표기】	조석헌
【성명의 영문표기】	CHO,SEOK HEON
【주민등록번호】	770127-1543416
【우편번호】	570-976
【주소】	전라북도 익산시 신동 775-21번지
【국적】	KR
발명자】	
【성명의 국문표기】	임선화
【성명의 영문표기】	LIM,SUN HWA

【주민등록번호】 700409-2095814
【우편번호】 302-793
【주소】 대전광역시 서구 월평동 주공아파트 207동 1004호
【국적】 KR
발명자】
【성명의 국문표기】 김영진
【성명의 영문표기】 KIM,YEONG JIN
【주민등록번호】 570808-1550312
【우편번호】 302-791
【주소】 대전광역시 서구 월평동 누리아파트 107동 1401호
【국적】 KR
발명자】
【성명의 국문표기】 안지환
【성명의 영문표기】 AHN,JEE HWAN
【주민등록번호】 560617-1460611
【우편번호】 305-804
【주소】 대전광역시 유성구 신성동 149-7번지
【국적】 KR
취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다.
대리인 유미특
허법인 (인)
수수료】
【기본출원료】 17 면 29,000 원
【가산출원료】 0 면 0 원
【우선권주장료】 0 건 0 원
【심사청구료】 0 항 0 원
【합계】 29,000 원
【감면사유】 정부출연연구기관
【감면후 수수료】 14,500 원
기술이전】
【기술양도】 희망
【실시권 허여】 희망
【기술지도】 희망
첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

IEEE 802.16에서 정의하는 Privacy 규격은 무선 네트워크로 구성된 tropolitan Area Network을 대상으로 SS(단말)에 대한 인증 기능을 규격화하고 있. 현재 이동서비스의 추세는 단말 또는 가입자의 이동성 지원이 필수 요구조건으로 타나고 있다. 이에 본 발명은 기 정의된 IEEE 802.16 규격의 인증 기능에 이동 가자 및 망간연동 시 요구되는 가입자 인증을 위한 방법을 제안하고 있다. 즉, 고정에서의 사용자 또는 단말의 인증은 이동 서비스를 이용하기에는 부가적으로 추가되야하는 기능들을 요구하여야하고, 본 발명은 이 요구사항을 해결하기 위한 방법이.

IEEE 802.16의 인증 규격을 정의하고 있는 Privacy 계층 규격에서는 단말(SS)와 기지국(BS)사이에 SS의 인증을 위하여 디지털 인증서를 이용하여 BS에서 적합한 가자인지를 확인하고, 인증키를 생성하여 전달하는 구조를 가지고 있다. BS는 액세스 장치로 SS와 연결된 네트워크 액세스 장치이다. 이동가입자가 해당망에서 서비스를 고자할 때 BS는 이 가입자에 대하여 적합성을 검증하여 주어야 하므로 이에 대한 하를 무시할 수 없다.

본 발명은 IEEE 802.16에서 정의하는 규격에 새로운 방법을 추가하는방법이다. 로이 제안하는 방법은 보안의 강도를 높여주고 SS의 이동성을 보장하도록 상위 계의 표준화된 프로토콜을 수용하는 방법이다. 제안하는 방법으로 현재 IEEE 802.16서 정의하는 MAC 규격에 기존의 인증 방법과 본 발명에서 제안하는 방법이 공존할 있도록IEEE 802.16 MAC 메시지인 SBC-REQ/RSP메시지에 인증 모드를 협상할 수 있

파라미터를 정의한다. 또한 본 발명에 따른 표준화된 인증 플랫폼인 EAP framework를 수용하기 위한 메시지를 MAC의 PKM 메시지에 추가로 정의하고, 해당 메시지에 필요한 파라미터를 제안하고 있다.

【표도】
도 6

【인어】

E. 프라이버시, SS

【명세서】

【발명의 명칭】

I E E E 802.16 프라이버시 계층에서 S S 인증을 위한 E A P 프레임워크 수용 방법(Acceptance method of EAP framework for SS authorization in IEEE 802.16 privacy layer)

【도면의 간단한 설명】

도 1은 본 발명이 적용된 IEEE 802.16에서의 SS 인증을 위한 시스템 구조도이다.

도 2는 본 발명이 적용된 IEEE 802.16에서 EAP기반의 SS 인증을 위한 MAC 연결 절차도이다.

도 3은 본 발명을 위한 IEEE 802.16에서 EAP기반의 SS 인증을 받기 위한 mac 인증 메시지 Flag 정보를 나타내는 도면이다.

도 4는 본 발명에 따른 IEEE 802.16에서의 EAP 기반의 SS 인증을 위한 MAC 흐름이다.

도 5는 본 발명에 따른 IEEE 802.16에서 EAP기반의 SS 인증을 위한 MAC 추가 메시지를 나타내는 도면이다.

도 6은 본 발명에 따른 EAP-trtansfer/EAP-transfer reply 메시지의 구성요소를 나타내는 도면이다.

도 7은 본 발명에 따른 SBC-REQ/SBC-RSP 메시지내의 authorization policy support 파라미터 포함방법을 나타내는 도면이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

본 발명은 IEEE 802.16의 SS 인증을 위한 기술에 관한 것이다. IEEE 802.16에서 정의하는 Authentication and authorization 규격은 무선 네트워크로 구성된 광대역 네트워크를 대상으로 단말에 대한 인증 기능을 규격화하고 있다. IEEE 802.16의 Privacy 계층으로 규격화하여 정의하고 있는 SS 인증기능은 현재 이동서비스의 추세인 단말 또는 가입자의 이동성 지원에 적합하지 않다. 즉 부가적으로 정의되어야 하는 요구사항들이 존재한다. 이에 본 발명은 기 정의된 IEEE 802.16 규격의 인증 기능을 이동 가입자의 인증을 위한 방법을 제안하고 있다. 즉, 고정망에서의 사용자 또는 단말의 인증은 이동 서비스를 이용하기에는 부가적으로 추가되어야하는 기능들을 정의하고, 해결하기 위한 방법을 제안한다.

SS 인증을 위한 종래 기술은 IEEE 802.16에서 정의하고 있는 MAC 계층에서 이루어지는 인증 기술로, 서로다른 사업자 망사이의 연동 서비스시 또는 SS의 이동서비스시에는 추가적인 정의가 요구되는 기술이다.

즉 고정망을 기반으로 SS의 인증을 위한 메시지 및 절차가 기술되어 있는 BS에의 구체적 기능들이 명시되어 있지 안하, 이동서비스를 위하여는 추가적으로 BS의 기능요구가 이루어져야한다. 추가적인 기능요구는 개략적으로 BS에서 guswo 서비스를 받는 모든가입자에 대한 프로파일을 갖고 있거나, 그렇지 않은 경우 CA인터페이스를 위한 API 또는 인증 서버와의 인터페이스를 위한 인증 클라이언트 수용등의 기능

요구한다. 또한 디지털 인증서 기반이므로, 인증서버에 접속하여 사용자 인증을
는 경우 반드시 인증서 기반의 인증을 수행하는 서버로 제한되며, 기존규격의 경우
와BS사이의 보안을 위한 키 분배를 BS에서 하도록 정의 되어 있어, BS 자체에 대한
안에도 또다른 향상된 기능이 필요하다.

발명이 이루고자 하는 기술적 과제】

본 발명에서는 IEEE 802.16에 SS의 인증을 위하여 표준화된 상위 인증 프로토콜
EAP framework인 EAP-TLS 또는 EAP-TTLS등을 수용하여 사용하는 방법이다.

이를 위하여 IEEE 802.16 MAC 메시지의 인증 메시지인 PKM(Privacy Key
nagement)메시지에 본 발명에서 제안하는 기능을 위한 메시지로 EAP-transfer
quest/reply 메시지를 추가하여야 한다. 또한 현재 정의되어 있는 IEEE 802.16
ivacy 기능과 본 발명에서 제안하는 방법이 공존을 하여야 하며, 이들 두 방법을
택적으로 선택하여 처리할 수 있도록 협상 기능을 두어야 한다. 이 협상을 위하여
Basic Capavility Negotiation request/reply (SBC-REQ/RSP) 메시지에 인증 방법
상을 위한 프래그(Falg)를 추가한다. 또한 본 발명에서 발생하는 메시지는 SS의 인
단계에서 수행되는 것으로 기존 규격에서 정의하고 있는 SS 인증의 기능을 보다
전하게 수행할 수 있다.

발명의 구성 및 작용】

본 발명은 IEEE 802.16의 privacy에서 SS의 인증을 위한 EAP 프레임 워크 수용
법이다.

도 1은 IEEE802.16에서 EAP 기반의 SS 인증을 위한 시스템 구조도이다. EAP 기
으로 SS의 인증을 수행하는 휴대인터넷망(101)은 가입자 단말 (Subscriber
ation: SS, 102), 기지국 (Base Station : BS, 103), 그리고 AAA서버
uthentication Authorization and Accounting Server, 104)로 구성한다. SS에서는
와의 통신을 시작하면서, SS자신을 인증받기 위한 인증 모드를 협상하고, 협상결과
따라 선택된 방법의 인증 절차를 수행한다.

기존의 IEEE 802.16에서 정의하는 privacy 기능으로 협상된 경우가 아닌 새롭게
안하는 본 발명의 기능으로 협상된 경우, SS와 BS는 EAP 기반의 인증 절차를 수행
기 위한 준비를 하며, SS는 EAP 메시지를 생성하고 이를 BS로 전달하여, BS에서 해
인증 서버와의 상호 작용을 통하여 자신을 인증받는다.

도 2는 EAP 기반으로 SS를 인증하기 위한 MAC에서의 연결 설정과정이다. 먼저
EE 802.16절차에 의하여 SS와 BS간의 인증 모드 협상을 위한 SBS-Request,
C-Reply 절차를 수행하고(201, 202) SS와 BS간에 협상결과에 따른 인증 모드가 설
된다.

본 발명에서 제안하는 EAP기반의 인증 보드로 선택된 경우, MAC 메시지 중 인증
시지인 PKM 메시지를 통하여 새롭게 추가한 EAP-transfer request와 EAP-transfer
ply메시지를 통하여 SS와 BS간에 인증 절차를 수행한다. (203, 204).

인증이 성공한 후, SS는 트래픽 보안을 위한 암호화 키를 요청하는 메시지인
y Request를 BS로 전달하고(205), BS는 해당 가입자가 요청한 키를 생성하여 Key
ply를 통하여 SS로 전달한다(206).

도 3은 EAP기반의 SS 인증 모드 선택을 위한 SBC-Request 메시지에 포함되는 플그(FLAG)정보이다.

ABC-REQ 메시지 Format(301)은 Management Message Type값으로 26을 가지며 02), TLV Encoded format(303)으로 파라미터의 융통성을 가진다. 포함될 수 있는 V로는 물리계층의 밴드위스 능력에 대한 협상을 위한 Bandwidth Allocation pport(304)와 본 발명에서 제안하는 인증 모드 선택을 위한 Authorization policy pport(305)를 비롯하여 physical parameter Support(306), 물리계층의 modulation, modulation관련한 협상 파라미터(307, 308), FFT 크기 협상을 위한 파라미터(309)을 포함한다.

도 4는 EAP 기반으로 SS를 인증하기 위한 MAC흐름도이다. 먼저 IEEE 802.16절차 의하여 SS와 BS간의 인증 모드 협상을 위한 SBS-Request, SBC-Reply 절차를 수행고(401) SS와 BS간에 협상결과에 따른 인증 모드가 설정된다.

본 발명에서 제안하는 EAP기반의 인증 보드로 선택된 경우, MAC 메시지 중 인증 시지인 PKM 메시지를 통하여 새롭게 추가한 EAP-transfer request 메시지내에 EAP 에 올라가는 응용 계층의 보안 프로토콜인 TLS또는 TTLS등의 데이터를 실어 BS로 달하고(402), BS에서는 MAC 메시지 중 인증 서버로 보내질 데이터를 추출하여 인증 버로 보내어(403), 그 결과 메시지를 받아(404), PKM메시지의 EAP-transfer reply 시지를 통하여 SS로 전달한다(405).

이러한 EAP-transfer request, EAP-transfer reply메시지는 EAP 기반의 상위 보 프로토콜에 의하여 사용자에 대한 인증이 인증절차가 완료될때까지 (402), (403), 04), (405)의 메시지를 반복하여 송 수신하며 인증절차를 수행하게 되고, 인증 단

의 마지막 절차에서는 SS가 요구한 EAP-transfer request(406)를 수신한 BS는 인증버로 이 데이터를 전송하고(407). 인증 서버로부터 결과를 받아(408) 인증 서버로터 해당 가입자의 인증 결과 성공이면 EAP-transfer reply 메시지에 해당가입자가용한 보안키를 생성하여 해당 키 관리를 위한 키 식별자. 라이프타임. SAID등과 함SS로 전달한다(409).

도 5는 본 발명의 결과에 따라 추가되어야 하는 IEEE 802.16 MAC 메시지 중 PKM시지에 추가되어야 하는 내용이다. 기존 메시지응 Code 3에서 12까지 정의되어 있. 본발명의 결과에 따른 메시지는 Code 13의 EAP-transfer request(501)로 SS에서로 전달되는 PKM-REQ메시지이와 Code 14인 EAP-transfer reply로 BS에서 SS로 전달는 PKM-RSP 메시지(502)이다.

도 6은 본 발명에 따라 추가된 메시지인 EAP-tranfer requestdhk EAP-transferply메시지에 포함되어야 하는 파라미터를 나타낸 것이다.

EAP-transfer request메시지에는 SS에서BS로 전송하는 메시지로 Securoty pability를 기술할 수 있는 파라미터이고(601). SS와 BS에서 보안 프로토콜을 운용여 통신하고자할 때 선택가능한 Security Association을 구분 할 수 있는 일련번호SAID(602). EAP 상위에 올라가는 사용자 인증을 위한 프로토콜용 데이터를 나타내EAP payload(603)을 포함한다.

EAP-transfer reply메시지는 BS에서 SS로 보내지는 메시지로 처리 결괄르 나타는 EAP Result code(604). 수행결과(EAP Result Code가 Failure)가 실패인 경우 SS서 취할 수 있는 에러 처리 기준을 제시해 주는 Error Code(605). 인증이

공한 경우 해당가입자에게 키를 분배하게 되고 이 키와 관련된 파라미터인 key "quence number(606), key lifetime(607)를 포함한다. 또한 SS와 BS에서 수용할 수는 시큐리티 셋에대한 설명을 나타내는 SA descriptor(608)과 상위 보안 프로토콜 데이터인 EAP Payload(609)를 포함 할 수 있다. 이들 파라미터 중, 인증 중간에 생하는Reply메시지에는 키 관련 파라미터는 포함되지 않고 인증 마지막 단계에서 증 결과 성공인 경우에만 키 관련 파라미터를 포함한다.

도 7은 SBC-REQ/RSP 메시지에 Authorization policy Support 파라미터의내용이 . Authorization policy Support 파라미터는 Bitmap 방식으로 비트 0는 IEEE 2.16에서 정의하고 있는 기존의 Privacy 모드(701)를 bit 1은 현재 제안하는 본발의 모드(702)를 나타낸다. 그외 비트는 현재 reserved되어 있으나(703), Bit 1이 텅된 경우, reserved되어 있는 Bit들을 사용하여 현재제공하는 상위 인증 플랫폼을 타내고자 한다. 구체적으로 Bit2는 EAP-TLS를 Bit 3는 EAP-TTLS를 나타내고(704) 후 지원가능한 응용 계층의 표준화 보안 프로토콜이 존재하게 되면 Bit4, bit5로 장가능하다.

정리하면, 본 발명에서는 IEEE 802.16에서 정의하는 Privacy 규격은 무선 네트크로 구성된 Metropolitan Area Network을 대상으로 SS(단말)에 대한 인증 기능을 격화하고 있다. 현재 이동서비스의 추세는 단말 또는 가입자의 이동성 지원이 필수 구조건으로 나타나고 있다. 이에 본 발명은 기 정의된 IEEE 802.16 규격의 인증 기에 이동 가입자 및 망간연동 시 요구되는 가입자 인증을 위한 방법을 제안하고 있 . 즉, 고정망에서의 사용자 또는 단말의 인증은 이동 서비스를 이용

기에는 부가적으로 추가되어야하는 기능들을 요구하여야하고. 본 발명은 이 요구사
을 해결하기 위한 방법이다.

IEEE 802.16의 인증 규격을 정의하고 있는 Privacy 계층 규격에서는 단말(SS)와
|지국(BS)사이에 SS의 인증을 위하여 디지털 인증서를 이용하여 BS에서 적합한 가
자인지를 확인하고. 인증키를 생성하여 전달하는 구조를 가지고 있다. BS는 액세스
장치로 SS와 연결된 네트워크 액세스 장치이다. 이동가입자가 해당망에서 서비스를
고자할 때 BS는 이 가입자에 대하여 적합성을 검증하여 주어야 하므로 이에 대한
하를 무시할 수 없다.

본 발명은 IEEE 802.16에서 정의하는 규격에 새로운 방법을 추가하는방법이다.
로이 제안하는 방법은 보안의 강도를 높여주고 SS의 이동성을 보장하도록 상위 계
의 표준화된 프로토콜을 수용하는 방법이다. 제안하는 방법으로 현재 IEEE 802.16
서 정의하는 MAC 규격에 기존의 인증 방법과 본 발명에서 제안하는 방법이 공존할
있도록IEEE 802.16 MAC 메시지인 SBC-REQ/RSP메시지에 인증 모드를 협상할 수 있
파라미터를 정의한다. 또한 본 발명에 따른 표준화된 인증 플랫폼인 EAP
amework를 수용하기 위한 메시지를 MAC의 PKM 메시지에 추가로 정의하고. 해당 메
지에 필요한 파라미터를 제안하고 있다.

발명의 효과】

본 발명의 효과는 IEEE 802.16에서 지원하는 SS 인증기능에 이동 SS에 대한 지
이 가능하고. 서로 다른 사업자 망들간에 연동 또는 동일 사업자이지만 서로 다른
으로 구성된 경우 이들 망간의 연동지원이 가능하다. 또한 표준화된 보안

로토콜을 지원하므로 확장성이 좋고, 안정성 면에서도 검증된 표준 보안 프로토콜

사용하므로 월등히 유리하다.

【특허청구범위】

【청구항 1】

IEEE802.16에서의 SS 인증 위한 시스템 구조를 도 1과 같이 구성하는 방법.

【청구항 2】

도 2와 같은 절차에서 SBC-REQ/SBC-RSP내에 authorization policy mode를 선택하는 방법.

【청구항 3】

청구항 2의 방법을 위하여 SBC-REQ/SBC-RSP내에 Authorization policy Support V를 추가하는 방법.

【청구항 4】

도 2와 같은 절차에서 IEEE 802.16 MAC 절차에 도 5와 같이 EAP-Transfer quest/reply메시지를 추가하는 방법.

【청구항 5】

청구항 2에 의한 메시지 구성에서 도 3과 같이 authorization policy support V를 구성하는 방법.

【청구항 6】

청구항 4에 의한 TLV를 추가하는 방법으로 도 7과 같이 비트 맵 방식으로 다양 상위 응용 보안 프로토콜을 지원하는 방법.

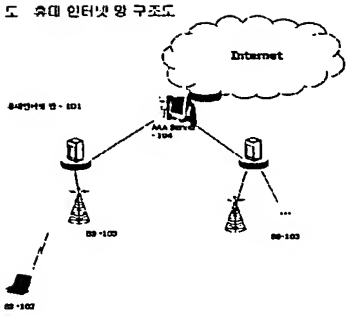
청구항 7]

청구항4에 의한 메시지 추가시 도 6과 같이 메시지 파라미터를 구성하는 방법.

【도면】

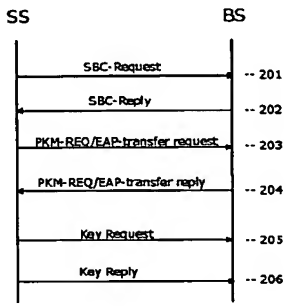
【도 1】

1도 휴대 인터넷 망 구조도



【도 2】

2 도. IEEE802.16에서 EAP기반의 SS 인증을 위한 위한 MAC 연결 절차도



[표 3]

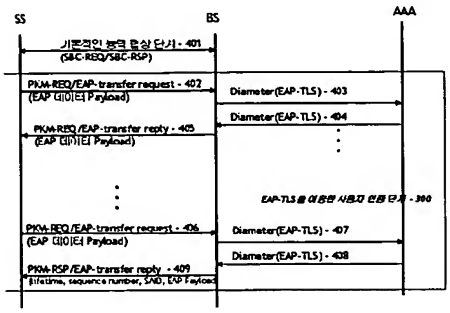
3 도. IEEE802.16에서 EAP기반의 SS 인증을 위한 MAC메시지 Flag 포맷

(표 48) - SS SBC-REQ Message Format

Syntax	Size	Notes
SBC-REQ_Message_Format() {		
Management Message Type = 36	8 bits	
TLV encoded information {	Variable	TLV specific
Bandwidth Allocation Support	0 bits	Bitmap 참조요망 (표
Authorization Policy Support	8 bits	Bitmap 참조요망 지정
Physical Parameters Supported {		
Demodulator	8 bits	Bit #0 = 64-QAM Support
Modulator	8 bits	Bit #0 = 64-QAM Support
FFT Sizes	8 bits	Bit #1 = FFT-2048
}		
}		
}		

[표 4]

4 도 IEEE802.16에 따른 IEEE 802.16에서의 EAP기반의 SS 인증을 위한 MAC 흐름도



[표 5]

5 도 IEEE802.16에서 EAP기반의 SS 인증을 위한 MAC 추가 메시지

Code	PKM Message Type	MAC Message Type
0 ~2	Reserved	
3	3A Add	PKM-RSP
4	Auth Request	PKM-REQ
5	Auth Reply	PKM-RSP
6	Auth Reject	PKM-RSP
7	Key Request	PKM-REQ
8	Key Reply	PKM-RSP
9	Key Reject	PKM-RSP
10	Auth Invalid	PKM-RSP
11	TEK Invalid	PKM-RSP
12	Auth Info	PKM-REQ
13	EAP-transfer Request	PKM-REQ
14	EAP-transfer Reply	PKM-RSP
15 ~ 255	reserved	

[표 6]

6 도. IEEE802.16에서 EAP기반의 SS 인증을 위한 EAP 메시지의 구성요소

EAP Transfer Request attributes

	Attribute	Contents
601	-Security-Capabilities	Describes requesting SS's security capabilities
602	-SAID	Security Association ID, being equal to the Basic CID
603	-EAP Payload	Contains the EAP-TLS Data, not interpreted in the MAC

EAP Transfer Reply attributes

	Attribute	Contents
604	-EAP Result Code	Describes success or failure
605	-Error Code	Error code identifying reason for rejection of authorization request.
606	-Key Sequence Number	Authorization key sequence number
607	-Key Life Time	Authorization key life time
608	-SA Descriptor	Specifies an SA ID and additional properties of the SA
609	-EAP Payload	Contains the EAP-TLS Data, not interpreted in the MAC

[표 7]

* 수. IEEE802.16e의 SBC-REQ/RSP 메시지의 Authorization policy support 파라미터 추가 방법

Type	Length	Value	Scope
5.21	1	bit #0 : 802.16 Privacy - 701 bit #1 : Open Privacy - 702 bit #2-7: *reserved*; shall be set to zero -703 (bit #2 : EAP-TLS, bit #3 : EAP-TTLS) -704	SBC-REQ (see 1.1.1.1.1) SBC-RSP (see 1.1.1.1.2)

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/KR04/002766

International filing date: 29 October 2004 (29.10.2004)

Document type: Certified copy of priority document

Document details: Country/Office: KR
Number: 10-2003-0076554
Filing date: 31 October 2003 (31.10.2003)

Date of receipt at the International Bureau: 12 November 2004 (12.11.2004)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse